REMARKS

Claims 1-22 are pending and stand rejected. In response, claims 1, 5, 9, 14, and 18 are amended and claims 7 and 16 are canceled. Claims 1-6, 8-15, and 17-22 remain pending upon entry of this amendment.

35 U.S.C. § 101 Rejections

Claims 5-13 stand rejected under 35 U.S.C. § 101 because the claimed invention is allegedly directed to non-statutory subject matter. Specifically, Examiner states that the language of the claims raises a question as to whether the claims are directed to merely an abstract idea and therefore do not produce a tangible result.

Applicants have amended the preamble of independent claim 5 to recite that the claimed method is performed by a computer. Moreover, Applicants submit that claims 5-13 produce the tangible result of adjusting authorized database accesses to deny database access operations by certain users. The claimed method is statutory at least because it recites the manipulation of data representing physical objects or activities (e.g., comparing actual accesses with authorized accesses) and is limited to a practical application in the technological arts (empirically adjusting access to a database). See MPEP 2106 IV.B.2.b.i and ii. If Examiner maintains this rejection, Applicants respectfully request that Examiner provide additional explanation of why the claim fails to comply with the statute.

35 U.S.C. § 102 and 103 Rejections

Claims 1-3, 5, 8, 9, 11-14, 17, 18, 20-22 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Mattson (US Patent Application Publication 2003/0101355A1). Further, claims 4, 10, and 19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Mattsson in view of Low et al. ("DIDAFIT: Detecting Intrusions in Databases through Fingerprinting Transactions"). Claims 6, 7, 15, and 16 stand rejected under § 103(a) as being unpatentable over Mattsson in view of Vaitzblit (US Patent Application Publication 2005/0097149A1). For purposes of clarity and simplicity, Applicants address these rejections together.

Independent claims 1, 5, and 14 are amended to recite denying database access for operations that were authorized but not observed. For example, amended claim 5 now recites:

> discovering authorized accesses to the database;
>
> observing actual accesses to the database;
>
> comparing actual accesses with authorized accesses; and
>
> adjusting authorized database access taking into account results of the comparing step to deny database access to operations by certain users on database tables and columns that **were authorized but were not observed** during the observation step.

Briefly, the claimed invention identifies instances where a user's authorized access to the database is broader than the accesses actually observed for the user. In response, the user's access is adjusted to deny access to parts of the database that were previously authorized but not accessed. Therefore, the threat of malicious activities is decreased because the scope of the user's authorized access is reduced. The features related to denying database access to operations that were authorized by not observed were previously recited by claims 7 and 16.

Examiner rejected claims 7 and 16 as obvious over Mattson in view of Vaitzblit. Generally, Mattson discloses a database intrusion detection system that uses inference patterns to detect intrusions. In Mattson, database access is controlled by security policies. Certain

sequences of accesses, although permitted by the security policies, may expose unauthorized information. Mattson's system detects these sequences, or inference patterns, generates alerts, and immediately alters user authorizations to make the accesses unauthorized. See paragraphs 34-37 and 46. Thus, Mattson's system adjusts the security policies based on **observed** accesses.

Vaitzblit, in turn, discloses a database audit system used to monitor, and optionally alert on database activity. Vaitzblit mentions in passing that audit reports it generates can be used to detect anomalies. The anomalies include a large number of accesses that resulted in permissions being denied and a change in data access patterns over time. See paragraph 19. However, Vaitzblit does not directly discuss detecting database intrusions or altering security policies based on monitored database activity.

Applicants respectfully submit that neither Mattson nor Vaitzblit discloses adjusting authorized database access based on operations that were authorized but **not observed**. Mattson makes inferences based on **observed** database accesses. Mattson neither teaches nor suggests denying database access based on accesses that were **not observed**. Vaitzblit, similarly, describes a way to audit **observed** database activity. Vaitzblit makes a general statement about how audit data can be analyzed to detect changes in data access patterns over time, but does not suggest denying database access based on accesses that were **not observed**.

Low discloses a database intrusion detection system that fingerprints SQL statements in order to detect illegitimate accesses. Low neither teaches nor suggests adjusting database access based on operations that were not observed.

Accordingly, Applicants respectfully submit that a person of ordinary skill in the art would not find the claimed invention obvious in view of the cited references and request that this application be allowed. The dependent claims not mentioned above are believed allowable at

least for incorporating the features of their base claims. Examiner is invited to contact the undersigned by telephone in order to advance the prosecution of this application.

Respectfully submitted,
HARLAN SEYMOUR ET AL.

Dated: November 22, 2006

By: /Robert A. Hulse/

Robert A. Hulse, Reg. No. 48,473
Attorney for Applicant
Fenwick & West LLP
801 California Street
Mountain View, CA 94041
Tel.: (415) 875-2300
Fax: (415) 281-1350